

[Show Modules](#)

Windows > Managing DNS on Active Directory

Managing DNS on Active Directory

[Dokumentasi CLI](#)[Back](#)[Next](#)

Managing DNS on Active Directory

Pada Active Directory, terdapat domain zone default yang akan dibuat saat proses instalasi Active Directory.

Saat menginstall Active Directory dengan domain **domain.local**, maka secara otomatis domain zone **domain.local** dan **_msdcs.domain.local** dengan tipe **Active Directory-Integrated Primary**

	Name	Type	Status
DNS			
WINSRV-01			
Forward Lookup Zones			
> _msdcs.domain.local	_msdcs.domain.local	Active Directory-Integrated Primary	Running
> domain.local	domain.local	Active Directory-Integrated Primary	Running
> Reverse Lookup Zones			
> Trust Points			
> Conditional Forwarders			

_msdcs.domain.local digunakan untuk menyimpan DNS record bertipe **SRV Records (Service Records)**. Record ini digunakan oleh client untuk menemukan **Domain Controller** dari domain.

Contoh pengecekan dari sisi client menggunakan perintah `nslookup` :

```

PS C:\Users\administrator> nslookup -type=SRV _ldap._tcp.dc._msdcs.domain.local
Server: UnKnown
Address: 192.168.17.173

_ldap._tcp.dc._msdcs.domain.local      SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = winsrv-01.domain.local
winsrv-01.domain.local internet address = 192.168.17.173
PS C:\Users\administrator>
PS C:\Users\administrator> nslookup -type=SRV _kerberos._tcp.dc._msdcs.domain.local
Server: UnKnown
Address: 192.168.17.173

_kerberos._tcp.dc._msdcs.domain.local  SRV service location:
    priority = 0
    weight   = 100
    port     = 88
    svr hostname = winsrv-01.domain.local
winsrv-01.domain.local internet address = 192.168.17.173
PS C:\Users\administrator>

```

Pada pengecekan diatas, dapat dilihat bahwa client akan melakukan lookup SRV records untuk menemukan service Active Directory seperti LDAP dan Kerberos. SRV record memiliki atribut **priority** dan **weight** yang digunakan oleh client untuk menentukan server mana yang akan dihubungi untuk service tertentu.

Penggunaan **SRV records** ini memungkinkan kondisi dimana satu windows domain memiliki lebih dari satu domain controller. Contohnya seperti berikut:

```

PS C:\Users\administrator> nslookup -type=SRV _ldap._tcp.dc._msdcs.domain.local
Server: UnKnown
Address: 192.168.17.173

_ldap._tcp.dc._msdcs.domain.local      SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = dc2.domain.local
_ldap._tcp.dc._msdcs.domain.local      SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = winsrv-01.domain.local
dc2.domain.local internet address = 192.168.17.174
winsrv-01.domain.local internet address = 192.168.17.173
PS C:\Users\administrator>
PS C:\Users\administrator> nslookup -type=SRV _kerberos._tcp.dc._msdcs.domain.local
Server: UnKnown
Address: 192.168.17.173

_kerberos._tcp.dc._msdcs.domain.local  SRV service location:
    priority = 0
    weight   = 100
    port     = 88
    svr hostname = dc2.domain.local
_kerberos._tcp.dc._msdcs.domain.local  SRV service location:
    priority = 0
    weight   = 100
    port     = 88
    svr hostname = winsrv-01.domain.local
dc2.domain.local internet address = 192.168.17.174
winsrv-01.domain.local internet address = 192.168.17.173
PS C:\Users\administrator>

```

Pada gambar diatas, **domain.local** memiliki dua Domain Controller (**winsrv-01** dan **dc2**) yang sama-sama menyediakan service LDAP dan Kerberos. Kedua SRV records tersebut

memiliki **priority** dan **weight** yang sama sehingga client dapat memilih salah satu domain controller (tidak ada preferensi).

Sedangkan zone **domain.local** digunakan untuk menyimpan DNS record umum seperti **NS, A, AAAA, CNAME dan lainnya**. Umumnya Administrator akan melakukan banyak konfigurasi DNS record pada zone ini.

DNS Zone Type on Windows

Pada DNS zone yang ada di Windows Server, terdapat beberapa tipe zone:

Select a zone type:

☒ Primary zone

Stores a copy of the zone that can be updated directly.

☐ Secondary zone

Stores a copy of an existing zone. This option helps balance the processing load of primary servers and provides fault tolerance.

☐ Stub zone

Stores a copy of a zone containing only NS, SOA, and possibly glue A records. A server containing a stub zone is not authoritative for that zone.

☒ Store the zone in Active Directory (available only if DNS server is a domain controller)

- **Primary:** Zone utama yang menyimpan DNS record secara read-write. Semua perubahan seperti penambahan, penghapusan, dan modifikasi record dilakukan pada zone ini.
- **Secondary:** Salinan (copy) dari primary zone yang bersifat read-only. Data diperoleh melalui proses zone transfer dari primary zone dan digunakan untuk redundansi serta distribusi beban query.
- **Stub:** Zone yang hanya menyimpan sebagian kecil informasi dari zone lain, seperti NS record, SOA, dan A record dari name server. Digunakan untuk membantu menemukan authoritative DNS server tanpa menyimpan seluruh isi zone. Mirip seperti forward.

Dari ketiga jenis diatas bisa dijadikan sebagai **Active Directory-Integrated** atau **Non Active Directory-Integrated**. Perbedaannya terletak pada lokasi penyimpanan DNS record.

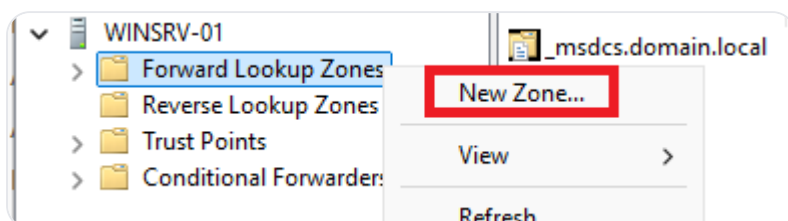
- Pada **Active Directory-Integrated**, DNS record disimpan di dalam database Active Directory (LDAP)
- Pada **Non Active Directory-Integrated**, DNS record disimpan dalam file, umumnya terletak disimpan pada direktori `C:\Windows\System32\dns`

DNS Zone Creation

Untuk membuat DNS zone pada Windows Server dapat menggunakan DNS management console `dnsmgmt.msc`. Di dalamnya terdapat **Forward Lookup Zone** dan **Reverse Lookup Zone**

Membuat Forward Lookup Zone

Klik kanan pada **Forward Lookup Zone**, lalu pilih **New Zone...**



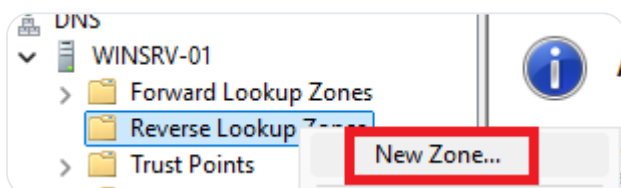
Pada bagian **Zone Type**, pilih tipe zone

Pada bagian **Zone Name**, masukan nama domain yang akan dibuat, misal `test.local`

Pada bagian **Dynamic Update**, sesuaikan dengan kebutuhan

Membuat Reverse Lookup Zone

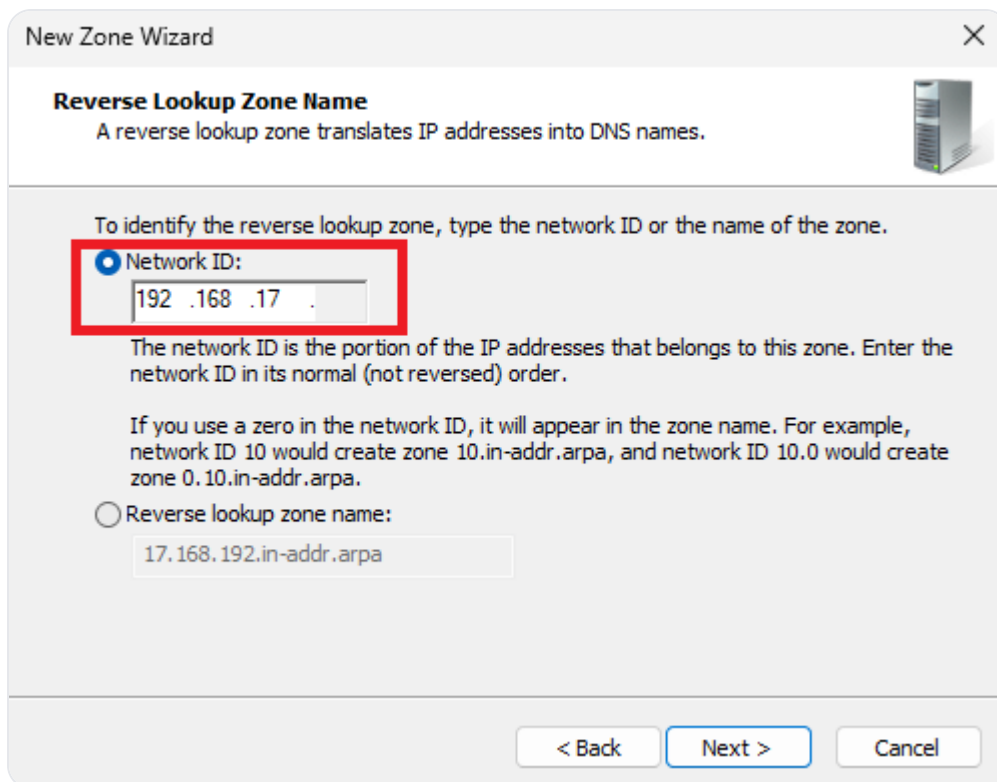
Klik kanan pada **Reverse Lookup Zone**, lalu pilih **New Zone...**



Pada bagian **Zone Type**, pilih tipe zone

Pada bagian **Reverse Lookup Zone Name**, pilih antara **IPv4** atau **IPv6**

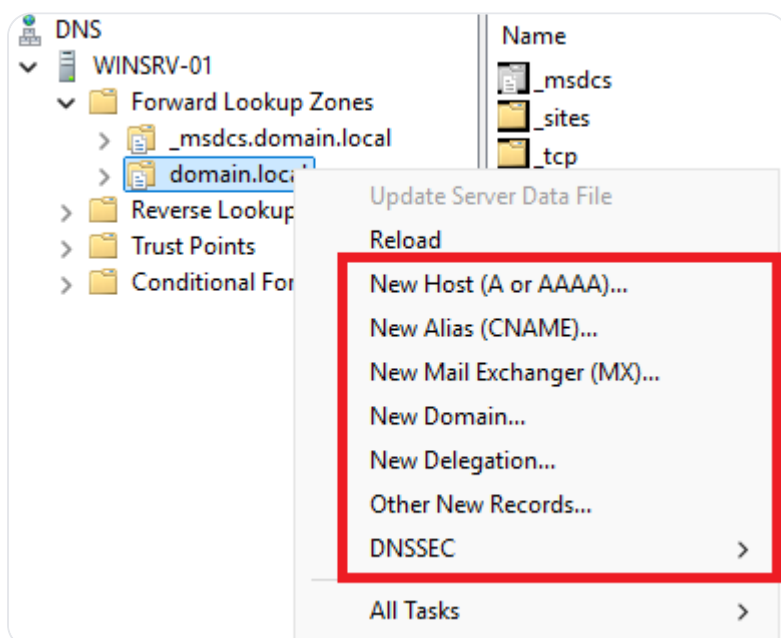
Pada bagian **Network ID**, masukan network address dari reverse lookup zone



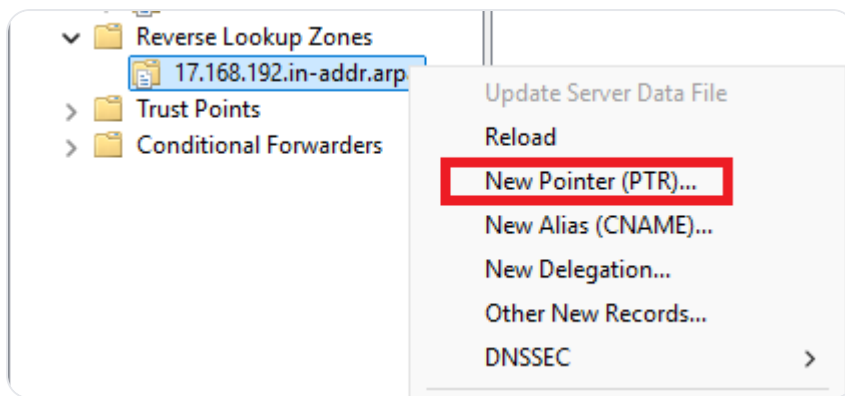
Pada bagian **Dynamic Update**, sesuaikan dengan kebutuhan

DNS Records

Untuk membuat DNS record, klik kanan pada zone lalu pilih beberapa salah satu record yang ingin dibuat, seperti A, AAAA, CNAME atau MX

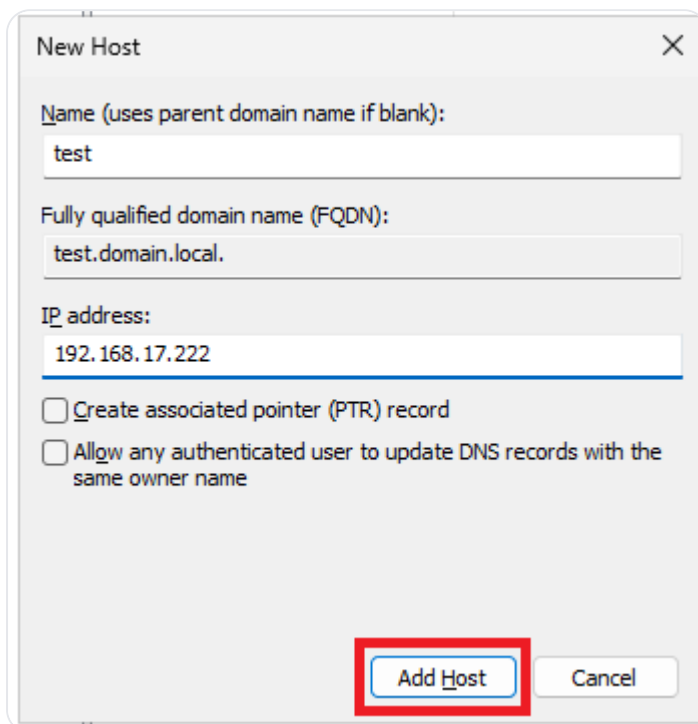


Begitu juga proses pembuatan record PTR pada reverse lookup zone:

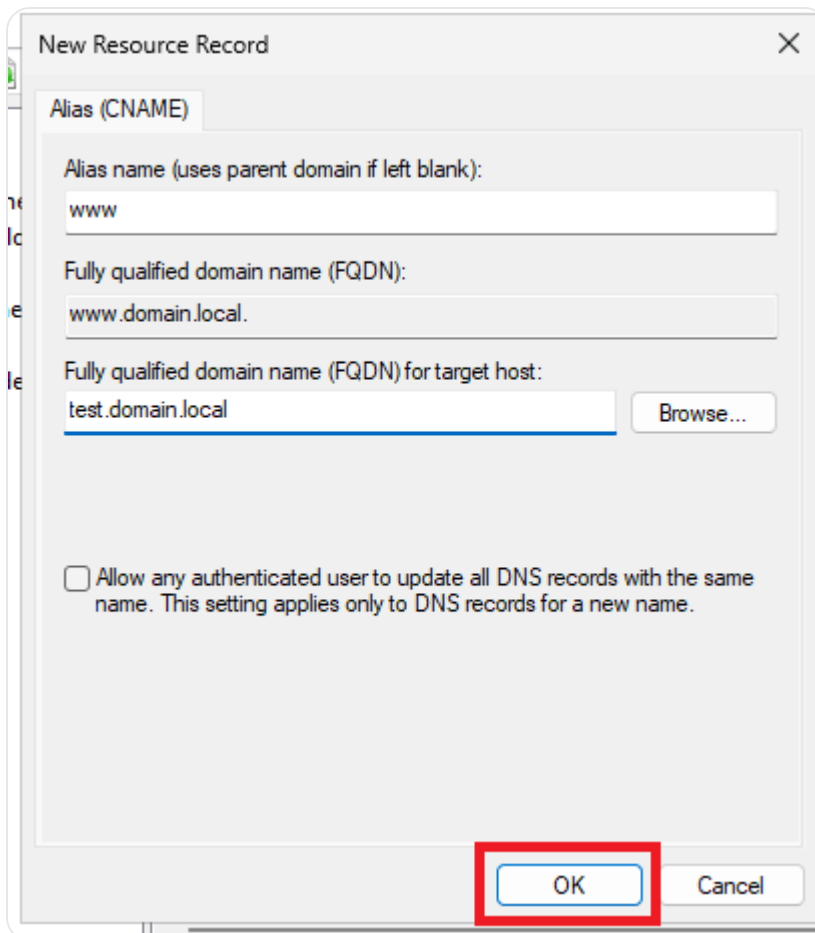


Contoh pembuatan beberapa record:

- **A record**

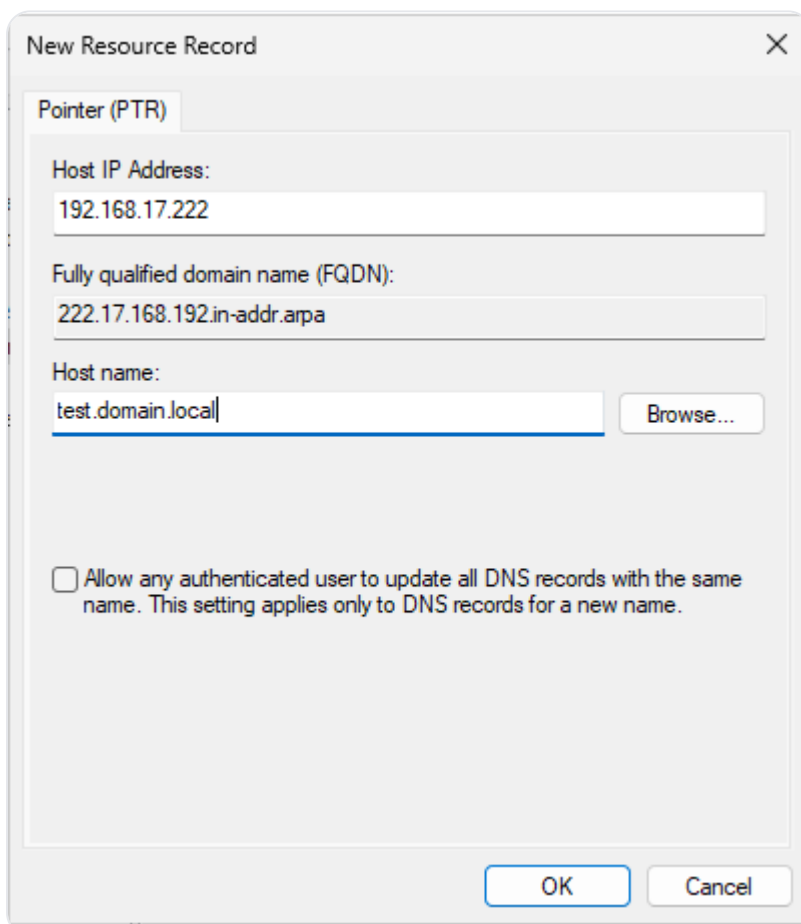


- **CNAME record**



The screenshot shows a 'New Resource Record' dialog box with the 'Alias (CNAME)' tab selected. The 'Alias name (uses parent domain if left blank):' field contains 'www'. The 'Fully qualified domain name (FQDN):' field contains 'www.domain.local.'. The 'Fully qualified domain name (FQDN) for target host:' field contains 'test.domain.local' and has a 'Browse...' button next to it. At the bottom, there is an unchecked checkbox labeled 'Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.' and two buttons: 'OK' (highlighted with a red rectangle) and 'Cancel'.

- **PTR record**

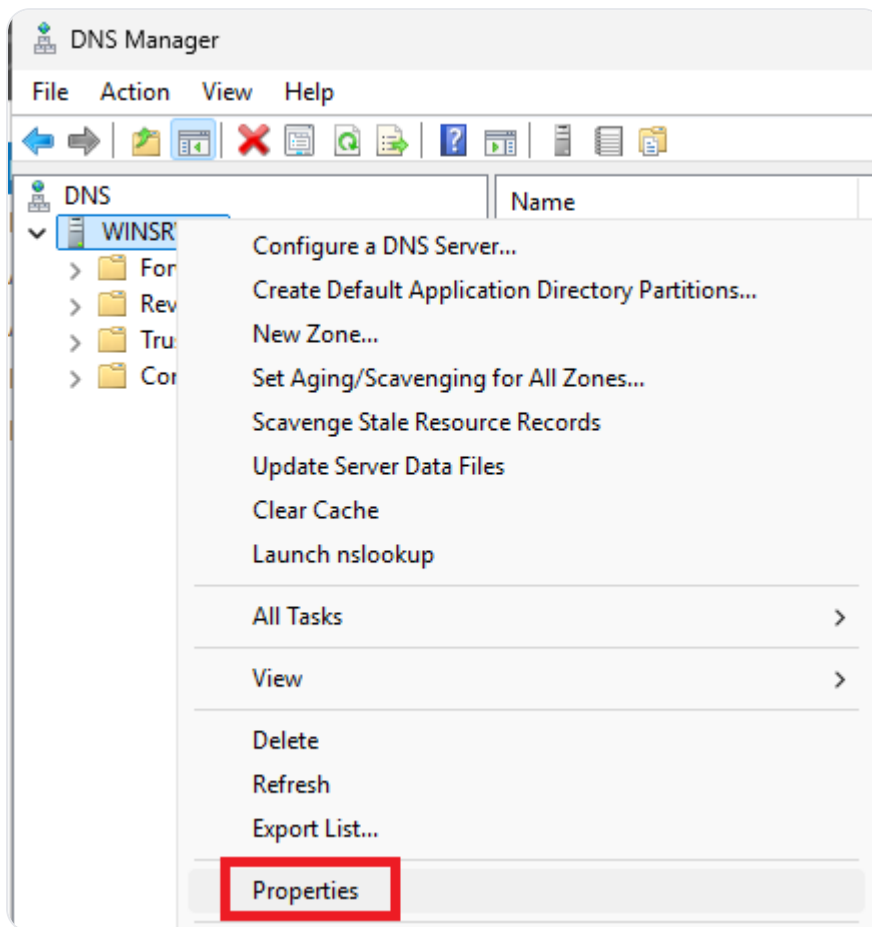


The screenshot shows a 'New Resource Record' dialog box with the 'Pointer (PTR)' tab selected. The 'Host IP Address:' field contains '192.168.17.222'. The 'Fully qualified domain name (FQDN):' field contains '222.17.168.192.in-addr.arpa'. The 'Host name:' field contains 'test.domain.local' and has a 'Browse...' button next to it. At the bottom, there is an unchecked checkbox labeled 'Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.' and two buttons: 'OK' and 'Cancel'.

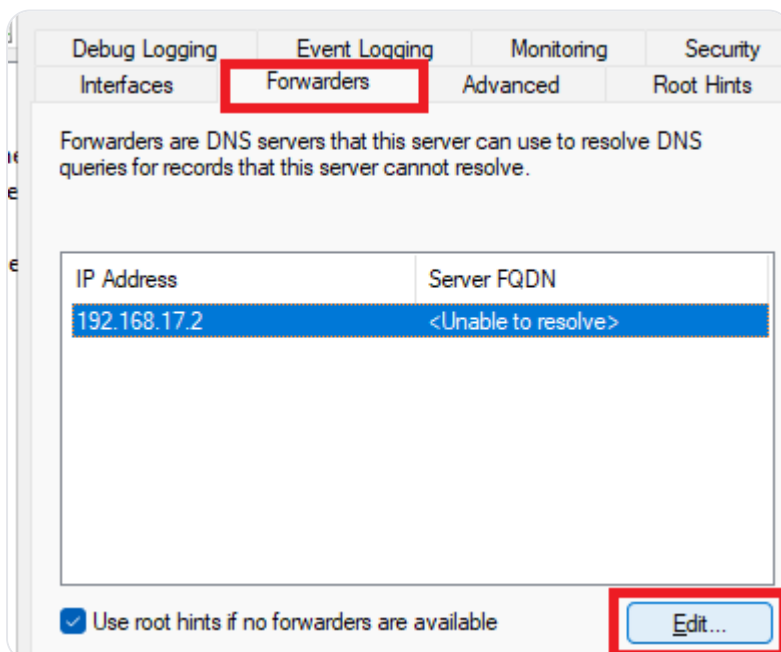
DNS Forwarders

Untuk konfigurasi DNS forwarders dapat dilakukan pada **dnsmgmt.msc** dengan langkah berikut:

Klik kanan pada server, pilih **Properties**



Pilih **Forwarders** lalu klik **Edit**



Tambahkan IP DNS server, contoh **1.1.1.1**, jika sudah klik **OK**

IP addresses of forwarding servers:

IP Address	Server FQDN	Validated
1.1.1.1		

Number of seconds before forward queries time out:

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

DNS Dynamic Updates

Dynamic Updates adalah mekanisme yang memungkinkan client atau host untuk menambahkan atau memperbarui DNS record (seperti A atau PTR) pada suatu domain zone.

Pada Windows Server terdapat beberapa tipe konfigurasi yang terkait Dynamic Updates:

- **None:** DNS server tidak mengizinkan DNS dynamic updates secara otomatis dari client.
- **Nonsecure and secure:** DNS server mengizinkan DNS dynamic updates baik dari client yang terautentikasi maupun yang tidak terautentikasi.
- **Secure:** DNS server hanya mengizinkan update dari client yang terautentikasi di Active Directory.

Secure dalam konteks Dynamic Updates ini artinya proses update DNS hanya dapat dilakukan oleh client atau komputer yang terautentikasi di Active Directory. Secara sederhana, Dynamic Updates hanya dapat dilakukan oleh client yang sudah join ke dalam Active Directory Domain

Mark Complete & Next